Information Technology
Induction Manual

Issued by Directorate of IT, ICSI
Version No.: V1.8

THE INSTITUTE OF
Company Secretaries of India
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

INFORMATION TECHNOLOGY
Induction Manual

Issued by Directorate of IT, ICSI
Version No.: V1.8

Document Information	
Process Name	ICSI IT Induction Manual
Document Owner	ISMS (Information Security Management System) Administrator
Document Number/Name	ICSI IT Induction Manual V 1.8
Document Approved by	CISO (Chief Information Security Officer)
Document Implemented by	Directorate of IT, ICSI
Implementation Date	19-11-2012

THE INSTITUTE OF
Company Secretaries of India
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

Headquarters
ICSI House, 22, Institutional Area, Lodi Road, New Delhi 110 003
tel 011- 4534 1000, 4150 4444 **fax** 24626727
email info@icsi.edu **website** www.icsi.edu / www.icsi.in

REVISION HISTORY					
VERSION NO.		RELEASE DATE	DETAILS OF CHANGES	REVIEWED BY	APPROVED BY
From	To				
D1.0	D1.0	16-10-2012	Initial Draft	CISO	
D1.0	V1.0	14-11-2012	First Release	ICSI	ICSI
V1.0	V1.1	24-11-2012	Review comments incorporated	ICSI	ICSI
V1.1	V1.2	06-06-2013	Review comments incorporated	ICSI	ICSI
V1.2	V1.3	07-08-2013	Review comments incorporated	ICSI	ICSI
V1.3	V1.4	29-10-2013	Review comments incorporated	ICSI	ICSI
V1.4	V1.5	17-02-2014	Review comments incorporated	ICSI	ICSI
V1.5	V1.6	24-06-2014	Review comments incorporated	ICSI	ICSI
V1.6	V1.7	15-09-2014	Review comments incorporated	ICSI	ICSI
V1.7	V1.8	19-12-2014	Review comments incorporated	ICSI	ICSI

TABLE OF CONTENTS

S. No.	Particulars	Page No.
I.	ELIGIBILITY TO USE INFORMATION RESOURCE POLICY	1
1	INTRODUCTION	1
2	SCOPE	1
3	ENTRY CRITERIA	1
4	INPUTS	1
5	ROLES AND RESPONSIBILITIES	1
5.1	All Personnel	1
5.2	Chief Information Security Officer	2
5.3	All HODs	2
5.4	System Administrators	2
6	POLICY	2
7	OUTPUT	3
8	EXIT CRITERIA	3
9	GUIDELINES, TEMPLATES	3
10	ISO 27001;2005 REFERENCE	3
II.	ACCEPTABLE USE OF IT RESOURCES POLICY	4
1	INTRODUCTION	4
2	SCOPE	4
3	ENTRY CRITERIA	4
4	INPUTS	4
5	ROLES AND RESPONSIBILITIES	4
6	POLICY	4
6.1	Ensuring Compliance	4

6.2 Acquisition of Hardware and Software 5
6.3 Complying with Copyright and Licensing 5
6.4 Using Personally Owned Software 5
6.5 Protecting Intellectual Property 5
6.6 Electronic Mail Messaging 5
6.7 Internet 6
6.8 Virtual Private Network (VPN) 7
6.9 Mobile Phones 7
6.10 E-Security 8
6.11 Authorised Monitoring 9
6.12 Security Violation 9
6.13 Security And Proprietary Information 9
6.14 Unacceptable Use 10
6.15 System and Network Activities 10
7 OUTPUT 11
8 EXIT CRITERIA 11
9 GUIDELINES 11
10 ISO 27001;2005 REFERENCE 15
III. INFORMATION TECHNOLOGY POLICIES OF THE INSTITUTE 24
IV GUIDELINES FOR THE USERS TO AVAIL IT RELATED SERVICES 33
V IT FACILITIES AND SERVICES FOR THE STAKEHOLDERS 35
VI UNIFORMITY NETWORK POLICY FOR RO/CCGRT/CHAPTERS 39
VII INTERNET USAGE GUIDELINE FOR USING THE INTERNET BY FACILITY EMPLOYEES IN RO/CCGRT/CHAPTERS 41
VIII Compliances for RO/CO/CCGRT (Points to note) 42
IX GUIDELINES RELATED TO BULK MAIL/SMS/WEBSITE UPDATION 43

I. ELIGIBILITY TO USE INFORMATION RESOURCE POLICY

1 Introduction

The use of Computers has become an essential part of most activities of an organization. While much computing is now done on privately controlled computers (PC, Desktop, workstation, Laptop etc.), most information sources and telecommunications systems reside on shared, central computers or use a shared network. These resources are owned/leased/rented by the organization and are provided primarily to enable/facilitate the official duties and responsibilities of the intended users.

This policy sets out the responsibilities and limitations on the use of ICSI's Information Processing Facilities (IPF) and the intention is to provide guidelines to avoid any unauthorized use of this information which may cause damage to the system, loss of data or criminal and/or civil liability for the User and/or ICSI. Personnel shall contact the Chief Information Security Officer (CISO) prior to engaging in any activities not explicitly covered by these guidelines.

2 Scope

This policy applies to employees, contractors, consultants, trainees, and other business partners Stakeholders in the data center, including all personnel affiliated to third parties.

3 Entry Criteria

- Hardware, Network and Applications are put in operation.
- Information Security Management System (ISMS) is established.

4 Inputs

- User profile
- Requirement to use the IPF (Information Processing Facilities)

5 Roles and Responsibilities

5.1 All Personnel

- Respective user approaches IT division with the request to use the IPF
- The request is recommended/approved by the respective group head

- Representative of IT division examines the request and grants / denies permission

All personnel shall be responsible for the following:

- Abiding by official corporate policies on acceptable use of information resources.
- Promptly reporting suspicion or occurrence of any unauthorized activities.
- Any use made of their accounts, logon IDs, passwords, PINs, and tokens

5.2 Chief Information Security Officer

The CISO (Chief Information Security Officer) shall be responsible for the following:

- Developing acceptable use policy for use of the IPF.
- Developing awareness and training materials.

5.3 All HOD's

HOD's at all levels shall be responsible for the following:

- Informing personnel of corporate policies on acceptable use of information processing facilities.
- Ensuring that personnel under their supervision comply with these policies and procedures.
- Ensuring that contract personnel under their supervision comply with these policies and procedures.

5.4 System Administrators

System administrators shall be responsible for the following:

- Monitoring systems for misuse.
- Promptly reporting suspicion or occurrence of any unauthorized activity

6 Policy

Access to the IPF by any user / 3rd party may be granted provided

- The request is accompanied by the reasons for the access, the name and contact information of the sponsoring official or administrator and the length of the time for which the access is required

- The request has been found to be commensurate with his responsibility
- In case of 3rd party user, the request is within the purview of the contract signed with the 3rd party.

Access to the IPF by any user / 3rd party may be denied or terminated:

- If the relationship of the user / 3rd party with ICSI is terminated
- If there is a concern for safety of systems or data out of usage of the specified user / 3rd party
- If there is reasonable belief that the individual to whom the access is assigned has perpetrated or is involved in illegal activities that violate any other policy of ICSI.
- If there is a written request from the Competent Authority including the HOD (Head of Division) / Vigilance or Internal Audit divisions as a part of an investigation of any misconduct / 3rd party in case of external user for removal of such access
- If unilaterally by ICSI, processes due to an unassigned user are causing or may cause damage to systems or data, or are causing or may cause serious service degradation for other users. Access may be restored after the threat is removed, unless other provisions of this policy are invoked.

7 Output

- Approval document to use the IPF (Information Processing Facilities)
- Provision in the IPF (Information Processing Facilities) for use by the user / 3rd party

8 Exit Criteria

- Confirmation / rejection communication to the user/3rd party.

9 Guidelines, Templates

- Available on Sharepoint Intranet Portal of the ICSI.

10 ISO 27001:2005 Reference

- A.7.1.3

II. ACCEPTABLE USE OF IT RESOURCES POLICY

1 Introduction

The Purpose of this policy is to outline the acceptable use of IT systems located physically and / or virtually at all premises, physical and / or virtual, owned and / or controlled by ICSI. This policy seeks to protect ICSI from vulnerabilities like inappropriate use of its information processing facilities (IPF) that may expose ICSI to risks.

2 Scope

This policy applies to employees, contractors, consultants, trainees and business partners in the data center and all electronic transactions of IT systems at DC, including all personnel affiliated to third parties.

3 Entry Criteria

- Hardware, Network and Application are put in operation
- Information Security Management System (ISMS) is established.

4 Inputs

- Approval document to use IT resource
- Provision in the IT resource to use by the user

5 Roles and Responsibilities

General use of Ownership – ICSI's IPF can be used for the following purposes

- Business purpose
- Regulatory purpose
- Control purpose
- R & D purpose
- Any other purpose with prior approval from Competent Authority

6 Policy

6.1 Ensuring Compliance

The organization owns all organization information processing facilities; the use of such facilities constitutes consent for the organization to monitor, inspect, audit, collect, and remove any information without permission or further notice. Personnel shall be trained in what use is acceptable and what is prohibited. Any violation

of organization acceptable use policies shall constitute a security violation for which personnel shall be held personally accountable and may be subject to disciplinary action or criminal prosecution.

6.2 Acquisition of Hardware and Software

To prevent the introduction of malicious code and protect the integrity of organization information resources, all hardware and software shall be obtained from official organization sources.

6.3 Complying with Copyright and Licensing

All software used on organization information processing facilities shall be procured in accordance with official organization policies and procedures, and shall be licensed & registered in the name of the Corporation. All personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

6.4 Using Personally Owned Software

To protect the integrity of the organization information processing facilities, personnel shall not use personally owned software on these resources. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally-owned or controlled software.

6.5 Protecting Intellectual Property

To ensure the integrity of organization developed software, all personnel shall abide by the intellectual property protection contract provisions of the corporation.

6.6 Electronic Mail Messaging

Access to the organization electronic mail (email) system is provided to personnel whose duties require them to have email for the conduct of organization business. Since email may be monitored, all personnel using organization resources for transmission or receipt of email shall have no expectation of privacy.

Acceptable Use

The organization provides email to facilitate the fast communication. Occasional and incidental personal email use shall be permitted if it does not interfere with the corporation's ability to perform its mission and

meets the conditions outlined in official organization directives. However, while they remain in the system, personal messages shall be considered to be in the possession and control of the corporation.

Prohibited Use

Prohibited activities when using organization electronic mail shall include, but not be limited to, sending or arranging to receive the following:

a) Information that violates state or central laws, or organization regulations.

b) Unsolicited commercial announcements or advertising material, unless approved by management in advance.

c) Any material that may defame, libel, abuse, embarrass, tarnish, present a bad image

6.7 Internet

Access to the Internet is available to employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of organization business. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy.

Acceptable Use

The corporation provides Internet access to facilitate the users to work effectively and efficiently. Occasional and incidental personal Internet use shall be permitted if it does not interfere with the work of personnel, the corporation's ability to perform its mission, and meets the conditions outlined in official organization directives.

Prohibited Use

Prohibited activities when using the Internet include, but are not limited to, the following:

a) Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the corporation has determined to be off-limits.

b) Posting, sending, or acquiring sexually explicit or sexually oriented material, hate based material, hacker-related material, or other material determined to be off-limits.

c) Posting or sending sensitive information outside of the corporation without management authorization.

d) Using other services available on the Internet, such as FTP or Telnet, on systems for which the user does not have an account, or on systems that have no guest or anonymous account for the service being used.

e) Using other services available on the Internet, such as FTP or Telnet, on systems for which the user does not have an account, or on systems that have no guest or anonymous account for the service being used.

f) Posting commercial announcements or advertising material.

g) Promoting or maintaining a personal or private business.

h) Receiving feeds and push data updates, unless the material is required for organization.

i) Using non-work related applications or software that occupy excess workstation or network processing time (e.g., processing in conjunction with screen savers).

6.8 Virtual Private Network (VPN)

a) It is responsibility of employees with VPN Privileges to ensure that unauthorized users are not allowed to access the organization's internal network.

b) All computers connected to the organization's internal network via VPN or any other technology must use the most up to date antivirus software that is the corporate standard, this includes personal computers.

c) By using VPN technology with personal equipment, users must understand that the machine is a defector extension of the organization's network and as such is subject to the same rules and regulations that apply to the organization owned equipment, i.e. their machines must be configured to comply with the organization's Security Policy.

6.9 Mobile Phones

a) While attending a call, try to maintain distance from others and use private place to attend personal calls whereas try not to take personal calls during business meetings, presentations or trainings etc.

b) Always speak softly, do not discuss personal or confidential business matters in public.

c) Do not get involved in other tasks while making calls and tell callers where you are, so that they can anticipate distractions/discussions.

d) Do not talk for a long duration if you are in face to face conversation with another person.

6.10 E-Security

a) Change temporary passwords at the first log-on.

b) Select quality passwords as per the Information Security Guidelines.

c) To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to Company's network must do so through an approved Internet firewall or other security device. If this is required for official reasons then permission must be sought explicitly from IT Department.

d) All hosts used by the employee that are connected to the organization's Internet/Intranet/Extranet, whether owned by the employee or the organization, shall be continually executing approved virus-scanning software with a current virus pattern/signature. In case Antivirus software is missing from user's PC and Server then IT should be informed immediately.

e) Port scanning or security scanning is strictly prohibited.

f) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty is prohibited.

g) Users are prohibited from using modems for inbound access to the organization's systems. In outbound dialup under certain cases where it is essentially required for official reason, permission from IT should be taken.

h) Personal chatting on internet is disallowed. In special cases, where chatting with external client is required, authorization is given by the project manager which is further approved by Head – Software Development.

6.11 Authorised Monitoring

a) While network administration of ICSI desires to provide a reasonable level of privacy, users should be aware that the assets, the users create in the IT system remains the property of ICSI. Because of the need to protect network of ICSI, the confidentiality of information stored on any network device belonging to ICSI can't be guaranteed.

b) Any user can be asked to provide usage details of their use of IT resources.

c) User shall be required to ensure that unattended IT systems allotted to him / her are given adequate and appropriate protection.

d) For security and network maintenance purposes, authorized individuals within ICSI may monitor IT systems and network traffic at any time with or without knowledge of the user.

e) ICSI reserves the right to audit network and IT systems on a periodic basis to ensure compliance of this policy

6.12 Security Violation

Violation of any security guidelines or policy mentioned in this document or elsewhere within ICSI or best practices would be considered as violation of security policy of ICSI and will be treated as unacceptable use.

6.13 Security and Proprietary Information

a) All users follow a formal authorization process before making any proprietary information, publicly available. The integrity of such information shall be protected after making it public also.

b) Special care to be taken for information stored in portable computers and storage devices.

c) All systems that are connected to the Internet / Intranet network of ICSI whether owned by employee /ICSI shall continually be executing approved virus-scanning software with current database in accordance with anti-virus policy.

d) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horse code, fishing information etc.

e) Employees must delete any spam (unsolicited bulk mail) mails received by them and should also avoid forwarding or originating any spam.

f) Exchange of proprietary information using other facilities including but not limited to voice, data, facsimile and video communication shall be controlled as per policy.

6.14 Unacceptable Use

a) All usages which are not for the purpose mentioned in the above or are in violation of any law of land are unacceptable.

b) All usage in violation of any policy of ICSI is unacceptable. However employees may be exempted from these restrictions for carrying out their assigned responsibilities (e.g. Systems Admin staff may have a need to disable the network access of a host during maintenance).

c) Under no circumstances, any user is authorized to be engaged in any activity that is illegal under local, state, central or international act or law while utilizing resources owned by ICSI.

6.15 System and Network Activities

TheThe following activities are strictly prohibited, with no exceptions:

a) Violations of rights of any person or company protected by copyright, trade secret, patent or other intellectual property right or similar laws or regulations, including but not limited to, the installation or distribution of 'pirated' or other software / products that are not appropriately licensed for use by ICSI.

b) Unauthorized copying of copyrighted material including but not limited to digitization and installation of any copyrighted software for which ICSI or the end user does not have an active license.

c) Introduction of malicious programs into the network or hosts or workstations.

d) Making fraudulent offers of products, items or services originating from any account of ICSI.

e) Effecting security breaches or disruptions of network communication. Here 'security breaches' includes, but not

limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these are within the scope of regular duties. Here 'disruption' includes, but not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

f) Port scanning or security scanning without prior notification IT division.

g) Executing any form of network monitoring which will intercept data not intended for the employee or his / her host, unless the activity is a part of the employee's normal activity.

h) Circumventing user authentication or security of any host, network or account.

i) Interfering with or denying service to any user other than the employee's host.

j) Any other activity using the IT Assets of ICSI that is detrimental to the interest of ICSI or is in contravention to the law of the land.

7 Output

Confirmation of communication to the users

8 Exit Criteria

All users have acknowledged the Policy

9 Guidelines

Information Security Guidelines

(i) General Guidelines

- Always save the data in another drive, not in root drive (generally root drive is C Drive).
- Always save your files on the Server Drive which is accessible to you only.
- Protect confidential files from unauthorized access through password protection.
- Back up critical data both at work and while traveling by using external disk/CD/Pen Drive etc.

- Backup should be checked at regular intervals - Daily/weekly/monthly.
- Don't open the services which are not required.
- Disable all the unnecessary auto runs.
- Delete temporary (temp) files on regular basis.
- Kindly lock your computer when you are NOT at your workstation – using CTRL + ALT + DEL.
- Power off the UPS after shutdown the Computer and before leaving the Office.

(ii) Password Security Guidelines

Password security guidelines are applicable to all services availed by the ICSI Users.

- List of don'ts with respect to passwords:
  - Don't reveal a password over the phone to ANYONE
  - Don't reveal a password in an email message.
  - Don't talk about a password in front of others
  - Don't hint at the format of a password (e.g., "my family name")
  - Don't reveal a password on questionnaires or security forms
  - Don't share a password with family members
  - Don't reveal a password to co-workers while on vacation
- Password Length should be minimum 8 characters.
- If someone demands a password, refer them to this document or have them call someone in the Information Technology Department.
- Do not use the "Remember Password" feature of applications (e.g., Eudora, Microsoft Outlook, Various Websites accessed using Internet Explorer or any other web browser).
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- Change passwords at least once every month.

- Use Strong passwords that have the following characteristics:
  - Contain both upper and lower case characters (e.g., a-z, A-Z)
  - Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
  - Is at least eight alphanumeric characters long
  - Is not a word in any language, slang, dialect, jargon, etc
  - Is not based on personal information, names of family, etc
- Example of a Strong password: 6reenLe@f

(iii) Internet Usage Guidelines

ICSI employees having access to the Internet on corporate network shall use it as a business tool and shall strictly follow these guidelines:

- The display of any kind of sexually explicit image or document on any ICSI system is expressly prohibited. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
- No employee may use ICSI facilities knowingly to download or distribute pirated software or data.
- No employee may use the ICSI's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap door program code.
- No employee may use the ICSI's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential information like employee information, customer data and trade secrets.
- Employees

1. with Internet access must not use ICSI Internet facilities to download software or games, or to play games against opponents over the Internet, download images or videos unless there is an explicit

business-related use for the material.

- Employees with Internet access may not upload any software licensed to ICSI or data owned or licensed by ICSI without explicit authorization from the manager responsible for the software or data.
- ICSI has installed firewalls, proxy servers, and Internet address screening programs to assure the safety and security of the Institute networks. Any employee who attempts to disable, defeat or circumvent any ICSI security facility will be subject to immediate dismissal.
- Employees are provided with internet access only for business purposes in interest of the institute. Any personal chats and other personal web emails, except ICSI provided emails are strictly prohibited.

(iv) Email Usage Guidelines

ICSI employees having access to the email on corporate network shall use it as a business tool and shall strictly follow these guidelines:

- Don't Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify IT Helpdesk.
- Don't Send unsolicited email messages.
- Don't Forge or attempt to forge email messages.
- Don't disguise or attempt to disguise your identity when sending mail.
- Don't send email messages using another person's email account.
- Do not send unnecessary attachments. Compress attachments larger than 1000 KB before sending them.
- Signatures must include your name, job title and company name. A disclaimer will be added underneath your signature.
- Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.

- Only mark emails as important if they really are important. It is strictly forbidden to use ICSI's email system for anything other than legitimate business purposes. Therefore, the sending of personal emails, chain letters, junk mail, jokes and executables is prohibited.

(v) Antivirus Security Guidelines

- Always keep your Anti-virus up-to-date.
- Never use any external USB media on your computer.
- Check all email attachments for viruses, worms etc. If one is not able to figure out, one must immediately contact the IT Team.

ISO 27001:2005 Reference

- A.7.1.3

(vi) Mobile Computing and Tele-working Process

Introduction

This process describes the procedure for handling Laptops, Notebooks, Mobile phones and any other transportable device in a secure manner. It also describes the procedure followed for Tele-working.

Entry Criteria

- Issue of a Laptop/Mobile Phones
- Requirement for Tele-working

Inputs

- Project requirements
- BCP test results

Roles and Responsibilities

IT Head is responsible for ensuring safe use of mobile computing and Tele-working facilities.

Tasks

Mobile Computing

Laptop allocation on a temporary basis

a) In case a laptop is required by any employee she/he may forward the requisition to IT Head, after approval from his/her Project Manager.

b) After approval of request, IT Head designates a member from the IT team to allocate the laptop.

c) The designated team member installs the required software, configures the network parameters and removes all redundant data from the laptop to be allocated.

d) The laptop is then handed over to the requestor and acknowledgement for receipt is taken.

Laptop allocation on a permanent basis

a) The steps as mentioned above for Laptop allocation on temporary basis are followed.

b) The Asset Register is updated accordingly.

Use of Personal Laptops

Use of personal laptops is allowed in ICSI premises with permission from the Head of the Directorate of IT.

Use of USB devices and unauthorized data cards are allowed in ICSI premises with the permission of Head of the Directorate of IT.

Use of Visitor Laptops

a) In case there is a visitor with a laptop, he may be allowed to enter into the office with the laptop with the permission of the Head of the Directorate of IT.

b) Visitor laptop is allowed to be connected to ICSI's network with the permission of the Head of the Directorate of IT.

Laptop de-allocation

a) When a user returns the laptop, she/he should ensure that the data has been backed up by him in any official storage device whose access has been given to him for use.

b) A designated person from the IT team ensures that the data is sanitized from the laptop before storing.

c) Material In/Out Register is updated accordingly

d) The allocation list maintained by IT is also updated.

Assignment of Admin Rights

a) All laptop users have been assigned administrative rights on their laptops to install and un-install necessary applications if required.

b) The user is responsible for ensuring legal compliance.

c) IT must be notified whenever such installation and un-installation is done.

Tele-working

a) Mails are accessible through Secured connections for the laptops and mobile handset users.

b) The organization provides VPN (Virtual Private Network) connectivity for Tele-working

- It is responsibility of employees with VPN (Virtual Private Network) Privileges to ensure that unauthorized users are not allowed to access the ICSI internal network.
- All computers connected to the ICSI internal network via VPN (Virtual Private Network) or any other technology must use the most up to date anti-virus software that is the corporate standard - this includes personal computers.
- VPN usage is allowed to all working for the Institute with the permission of the Head of the Directorate of IT.

Output

- Updated Laptop Users list
- List of authorized VPN (Virtual Private Network) Users

Exit Criteria

- Laptop is issued
- Return of an issued laptop
- VPN access to the identified and approved users

Guidelines, Templates

- Laptop Security Guidelines

  IT Change Request Form with VPN (Virtual Private Network) Authorization

ISO 27001:2005 Reference

- A.11.7.1, A.11.7.2

(vii) Physical and Environmental Security Process

Introduction

The physical and environmental security of an organization includes the measures taken to safeguard the physical infrastructure of the organization. It also includes measures taken to protect the organization from environmental hazards.

Entry Criteria

Operations running within the organization's premises.

Inputs

- Project requirements
- BCP test results

Roles and Responsibilities

ISMS (Information Security Management System) Administrator: Setting up the Business Continuity Management team

Security Committees: Review of Business Continuity Plan

Individual project managers: Capturing the business continuity needs of their projects and communicating to Business Continuity coordinator

Tasks

Secure areas

Access to the premises is restricted. The premise is divided into three categories: Secure zone, Controlled zone and unrestricted zone.

Secure zone

- This area includes those server rooms and project areas that have been classified as critical or sensitive. This area is provided maximum security, with different levels of authentication like biometric identification and access control cards.
- Only authorized personnel can access this area. Third party contractors and vendors who need to enter the secure zone must always be escorted by authorized personnel and remain escorted during the course of their stay in the server room.

- Visitor information is recorded in Visitor Entry Register and a temporary access card is provided.

Controlled zone

This area includes the work area of the employees, and is restricted to internal employees, and authorized set of contract personnel like cleaning, catering, maintenance etc. Access to this area is through access control cards only.

Unrestricted zone

This zone includes the common areas like reception, waiting rooms, lounge, etc, where visitors, temporary/permanent access cardholders can visit.

Physical Entry Controls

Appropriate physical entry controls are implemented in the organization. Access control cards are issued by the Admin manager after getting duly signed authorization requests for issuance of cards from the Admin head, to the following:

Employees

The access card database is updated with the access card number, date of issuance and validity date. Access card for employees is identified by blue colour.

Third party contract employees/Trainees

They are given temporary access cards till the date of validity of their contract with the organization. The access card database is updated with the access card number, date of issuance and validity date. Access card for Third Party/ Trainees is identified by green colour.

Security Personnel/ Housekeeping

They are issued access control cards with a black colour.

Visitors

They are given visitor card by the security guard after getting authorization from the organization employee whom they have come to visit. The visitor register is updated with the name, time of issuance and card number. The card is returned by the visitor to the guard before leaving the premises and the visitor register is again updated.

Access Card Management

Access cards are issued by the Admin manager after due authorization from the Admin Head.

The mapping between employee code and access card no issued to him is stored in the access card database.

At the time of an employee leaving, the access card is returned to the Admin manager.

Temporary cards do not have access to any secure zones. The employee has to return the card before leaving for the day.

The Admin head or a person designated by him does a review of the access rights to all secure zones once a quarter. The existing rights are verified with the respective Project Manager.

Guidelines for Physical Access

a) All the employees must wear the access control cards on their person throughout their stay in the organization premises.

b) Security inspection is done at all entry and exit points in the organization.

c) If any access card is lost, it must be reported immediately to the HR (Human Resource) Executive. Random and on the spot checks are done by Administration department to assess the security awareness of the personnel.

Protection from Fire

a) The organization is well protected from fire by fire extinguishers, smoke detectors and water sprinklers installed at appropriate locations.

b) Fire alarms are installed at appropriate locations.

c) The equipment is maintained as per the instructions by vendor.

d) Fire drills are held every quarter and a report of the same is sent to the senior management.

e) All fire exits are clearly indicated.

f) Fire extinguishers are properly labeled and installed at all ICSI event locations.

g) Explicit instructions are boldly and clearly written for the safe evacuation of personnel in the event of a disaster.

Equipment Security

Equipment must be appropriately protected to minimize the risks of environmental threats. The following procedure is followed:

a) Any organization equipment that goes out of the premises must be accompanied with an authorized letter from authorized person. It must be entered in the outgoing equipment register.

b) Any equipment like systems, security devices, etc., that are brought into the premises, are first entered in the Inward register. The admin group ensures that the equipment is safe before authorizing its entry into the loading area. The Fixed Asset Register is updated for any new or modified equipment.

c) Power or electrical and data cables are routed through separate paths.

d) Temperature needed is appropriately controlled in the server room. The humidity check is not done since Air Conditioner is available round the clock.

e) All organization equipment is protected from power outages by dedicated generators and UPS. Servers also have dedicated UPS.

f) Quarterly checks of the power supply backups are carried out as per the SLA with the concerned Service Providers.

g) The construction of the building is as per the regulatory requirements.

h) EPABX is installed at the reception and access is given only to the receptionists who are authorized by the admin group. The configuration of the EPABX system is as per the rules set by the management in accordance with the security policy. During non-working hours the calls are logged in the voice box.

i) Please refer to Guidelines for EPABX security.

Output

- Issued access control cards
- Logs of physical access control

Exit Criteria

- It is a continuous process in the organization

Guidelines, Templates

- Guidelines for EPABX Security

ISO 27001:2005 Reference

A.9.1.1, A.9.1.2, A9.1.3, A.9.1.4, A.9.1.5, A.9.1.6, A.9.2.7

(viii) User Registration and De-Registration Process

Purpose

The purpose of this procedure is to describe the user registration and de-registration process in ICSI. This procedure addresses the following:

- User Access Management
- User ID Management
- Password Management
- Privileged User ID and Password Management

Scope

This procedure is applicable to all the logical access provided within ICSI.

Procedure

Access Approval Process

An access request form (Request for Access Creation / Modification / Disabling / Deletion Form) shall be made available for users. The process for providing access to various IT resources such as user IDs shall be as follows:

- Access is requested by the Associate Head /Supervisors
- All Associate Head /Supervisors shall forward the same to the signing authority in IT Dept., who would approve or reject the request.
- IT & System team shall take necessary steps (create ID and password, etc.) and inform the initiator of the request of the same.
- The nominated personnel shall update the records and file the request form.

Access Deletion process

The request for the disabling or deletion of account must be made in the following manner:

- Email from Department Head/Associate Head/Supervisors IT Dept, with detailed reason for deletion/disabling of user ID.
- Email from HR department to IT Department with detailed reason for deletion/disabling of user ID.
- On termination / Superannuation / Resignation of the official from the services of the Organisation and on issue of the office order by HR department.
- IT & System team will disable the user ID.

- IT & System team will backup requested information of terminated/relived employees as per respective department head.

In case of disabling:

- Nominated system administrator would disable the user ID and update the user ID database with the status of the user ID.
- The nominated system administrator shall file the request and inform the respective process owner.

Roles and Responsibilities

Role	Responsibility
HR Department	a) Requests for new joiner user id creation b) Requests for user id deletion/ disabling c) Intimation of all transfers/exits/deputation movement of employees
IT Dept.	a) Requests for new joined authorizations b) Requests for user id deletion/ disabling c) Approves user access creation/ modification/ disabling/ deletion
User	a) Request for Change of Access on any system to their Associate Heads/Supervisors

Point Of Contact

- Chief Information Security Officer /Designated Authority

ISO 27001:2005 Reference

A.11.2.4, A.12.1.1

III. INFORMATION TECHNOLOGY POLICIES OF THE INSTITUTE

Sl. No.	Related to	Policy
1.	Hardware Replacement in HQ/RO/Chapters	All the hardware (server, desktop, printer, Scanner, UPS, Router, Switches, Fire wall etc.) may be replaced in HQ/RO/ Chapters under buyback on the completion of 5 years. The above policy will be effective with immediate effect.
2.	Provision of Hardware to RO/Chapters	All Chapters would be provided with Computers, Printers and UPS provided they have their own offices and/or operating from rented premises. Laptop, LCD Projector would be provided to all Regional Councils, A+, A, B, and C Grade Chapters provided they have their own offices and/or operating from rented premises. Request / requirement of D Grade chapters shall be considered on need basis provided they have their own offices and/or operating from a rented premise.
3.	Provision of Hardware for the Staff in HQ/RO/ Chapters	Desktop will be provided to every regular staff starting from Junior Assistant level onwards working in HQ/RO/Chapters on 1:1 (staff : computer) basis. Printer will be provided to the directorate / RO / Chapters on 3:1 (staff : printer) basis. Scanner will be provided to the directorates on 1:1 (directorate : scanner) basis. Any hardware requirement of the directorates outside the mentioned policy may be fulfilled with the approval of the Chief Executive OR Secretary subject to the availability of the budget.

		Note: As per Directorate of HR - 1. Specified Staff A is not to be provided email id and therefore desktop is also not to be provided. 2. Specified Staff B is to be provided email id and therefore desktop is also to be provided.
4.	Software	Only licensed software's are to be used in the Institute's HQ/RO/Chapters. As per standard in practice Software's such as MS Office 2003/2007, MS Outlook 2007, Internet Explorer 8/9 and OS Windows XP Professional/2007/2008 are in use. To ensure that software licensing policy is being practiced properly, the Institute will get the software usage evaluated by the Facility Management Service (FMS) firm, who is responsible for Data Center and System Administration for the HQ once every year and accordingly fulfill the shortage of licenses, if any through procurements. In case of RO/Chapters, the In-charge of the respective branch office will be liable to ensure the compliance of the software licensing policy. RO/Chapters will submit a self-declaration certificate in the format as approved by the IT Committee stating that their office is using only the licensed software. This declaration certificate is to be submitted every year in the month of January by all RO/Chapter/CCGRT offices. RO/Chapters on request may receive the approval from HQ for procuring the software license for Anti-Virus and MS Office (Academic version only) and then procure the same themselves by following the purchase procedure of the Institute and get the limited reimbursement to that effect.

5.	Bulk Mailing request by directorate/ RO/Chapters	All bulk mailing requests from the directorates / ROs / Chapters must come directly to the Directorate of the IT of the Institute. The request must be sent to the Directorate of IT at least 3 working days before the program. RO/Chapters will reimburse the bulk mailing charges to the HQ on actual usage basis and on actual bulk mailing charges being paid to the third party. As per practice, the bulk mailing services is utilized for Professional Development Activities and Student Services. In addition to the same, bulk mailing shall be allowed for Republic / Independence Day / Birthday of Mahatma Gandhi.
6.	Bulk SMS request by directorate/ RO/ Chapters	All bulk SMS request from the directorate / RO / Chapters must come directly to the Directorate of IT of the Institute. The request must be sent to the Directorate of IT at least 3 working days before the program. RO/Chapters will reimburse the bulk SMS charges to the HQ on actual usage basis and on actual bulk SMS charges being paid to the third party. Maximum characters, that may be sent by SMS is 160 characters. As per practice, the bulk SMS service is utilized for Professional Development Activities and Student Services. In addition to the same, bulk SMS shall be allowed for Republic / Independence Day / Birthday of Mahatma Gandhi.
7.	Policy for IT Committee at RO/Chapters	1. The IT Committee will comprise of office bearers of ROs/Chapters. Outside experts may also be taken in the Committee as advisory members. Number of members in the IT Committee is to be at least 3 and not more than 5. The IT Committee in ROs may be formed by the Regional Council whereas in the Chapter by the Managing Committee.

		2. The IT Committee must meet at least once in every quarter. Special meetings may be convened, if required with the permission of the Chairman of the Committee. 3. Recommendations of the IT Committee of RO/Chapters should be sent to the IT Committee of the Central Council after the same is considered and approved by the Regional Council / Managing Committee. 4. The Committee will explore the areas/applications where computerization is feasible and provide suggestions with sufficient justifications. 5. The IT Committee will identify the resources in terms of hardware, software, manpower and other infrastructure requirements for the proposed computerization as per the areas mentioned in serial no. (4). 6. The IT Committee will recommend for the purchase of hardware and software required for the computerization of that RO/Chapter, which will be forwarded to the IT Committee of the Central Council after the same is approved by the Regional Council / Managing Committee. 7. The IT Committee will monitor the complete computerization process of the respective RO/Chapter including the implementation of software provided by HQ. 8. The IT Committee will monitor the updations and management of the child portal of the RO/Chapter (Eg; for WIRC it is www.icsi.edu/wirc). 9. The IT Committee will ensure that the networking / chat & email facilities have been implemented at RO / Chapter and monitor the same on monthly basis. 10. The IT Committee will take initiative to get more and more data of the members such

		as email and phone numbers, which can be utilized for sending bulk email and SMS respectively. 11. The IT Committee will ensure that the utilizations of services offered by the Head office are being properly utilized by the RO / Chapter such as : (a) SMS message to members of that region / chapter (b) Advice on Hardware and Software and legal implications of software (c) Maintenance of web site (d) E-mail facility on icsi.edu (e) Bulk Email 12. The IT Committee will ensure the following for the respective RO / Chapter: (a) The hardware is under proper AMC and is being upgraded from time to time. (b) All the computers are protected from virus attack. (c) Only licensed software being utilized. (d) The software licenses are kept in safe custody and can be made available at all times. (e) A proper internet connection is available in the RO/Chapter for effective communication. 13. The IT Committee will monitor the ensuing timely entry of credit hours and facilitate the online services to students like online registration, online admit cards, online result etc.
8.	MIS Report submission by RO/ Chapters	MIS report in the prescribed format (as prescribed by the Directorate of IT of the ICSI) is expected from Regional and Chapter Offices by 7th of every month.

9.	Email Ids for Chairman/ Secretary of RO/Chapters	Separate email IDs may be allotted to the Chairman and Secretary of all the RCs and Chapters on icsi.edu domain. The extract of the minutes are as follows : "The Committee approved creation of separate email IDs for Chairman and Secretary of all the Regional Councils and Chapters on icsi.edu domain. The structure of email IDs for Regional Council would be like chairman.eirc@icsi.edu; secretary.eirc@icsi.edu. The structure of email for Chapter would be like chairman.nagpur@icsi.edu; secretary.nagpur@icsi.edu. The committee advised that these email IDs be created within shortest possible time. The committee further advised that such email IDs for Regional Councils and Chapters be made available only upon getting the undertaking as approved by the IT Committee from the respective users. The password for email IDs given to the Chairman and the Secretary of RCs and Chapters must be deactivated by the IT department on expiry of respective terms of the Office (i.e. from 19th January to 18th January) without any further reference."
10.	Hardware Specification	Different computer / laptop configuration may be procured according to user profile. For example superior configuration for Officers handling software development and network monitoring and standard configuration for other users.
11.	Procurement of Hardware for RO/Chapters	RO/Chapters will procure the hardware of their own following the prevailing purchase policy of the Institute and claim the reimbursement.
12.	IT Security Policy	All the users will follow the IT security policies as is being practised and propagated by the Directorate of IT from time to time. All the users are required to fill the prescribed form for availing the facilities pertaining to privileges for accessing the systems / data / applications / emailing services etc.

		Currently, the Institute is implementing the IT security policies as has been approved by the IT Committee of the Institute in its 35th Meeting held on 7th November, 2012.
13.	Data Sharing Policy	As per the decision taken in **216th meeting of the Council held on 21st and 22nd June, 2013, the data sharing policy is as under:** a) The data relating to students, namely, postal address, e-mail and telephone number, shall not be shared with anyone. b) The postal address of members may be shared with everyone on request. c) The register of members shall carry the details as required under the Act. d) The list of members published (in paper or electronic form) by Institute may be available to everybody on request. This list will carry the prescribed details, including postal address. This list will not carry e-mail address and telephone numbers of those members who do not wish these details to be published. e) The IT Department will facilitate ROs/COs/Directorates to send mails/messages to identified groups of members/students, but they would not have access to these details. f) In case, it is required to share the data with any third party handling the jobs pertaining to the stakeholder's data in the area where Institute does not have the requisite infrastructure and manpower, the Non-Disclosure Agreement must be signed. **Latest Developments:** Further As per the decision taken in **224th meeting of the Council held on 12th and 13th June, 2014, the data sharing policy (additional) is as under:** The Council decided that the contact details of students covered in the jurisdiction of a CO or RO, as the case may be, may be provided to

		respective RO or CO on demand from them if they are conducting oral coaching classes and give an undertaking that they would maintain confidentiality of the data.
14.	Policy for Bulk SMS and Bulk Mailing	Finance Committee in its 26th meeting held on 23rd June 2014 has decided as under: - "The Committee advised that bulk SMS and bulk E-mail must be restricted to the concerned Region / Chapter / location to which it concerns. It should not be sent to all the members of the Institute."
15.	Policy to provide obsolete hardware to the employees of the Institute at cost	1. Only computer's CPU, monitor, Keyboard and Mouse (as is available) will be offered to the employees under this policy. 2. The list of obsolete computers (CPU only) to be sold under buy back will be published on the Institute's intranet i.e. http://cosmic. The list will have the details such as hardware name, configurations, status of the hardware (In use/Not in use), Department where it is being presently used, User Name etc. 3. The interested employee may be requested to submit their requisition to procure any of the computers from the list. 4. In case more than one employee gives requisition to procure a particular computer, the employee will be selected thru lucky draw. 5. As the cost of a computer under buy back on the previous occasions has been noted as maximum of Rs.2000/-, it is suggested that the cost of these obsolete computers may be kept as Rs.2000/- (fixed) irrespective of the configurations. 6. The Secretariat should take a firm commitment of the employee that the computer provided will not be sold for a period of three months from the date of procurement. 7. Only one computer shall be provided to one staff employee.

Policies in Practice in the Institute:

S. No.	Related to	Policy
1.	Anti-Virus	Every Office of the Institute of its own will procure and install suitable Anti-Virus software in all the desktops/Laptops. For the offices which are connected under Wide Area Network, this responsibility lies with the ICSI HQ. RO/Chapters may also send their request to HQ for sanction order to procure antivirus software and then procure themselves by following the purchase procedure of the Institute and get the limited reimbursement to that effect.
2.	Office Automation Software	Every Office of the Institute of its own will procure and implement MS Office as the standard Office Automation Software. RO/Chapters may also send their request to HQ for sanction order to procure MS Office software and then procure themselves by following the purchase procedure of the Institute and get the limited reimbursement to that effect.
3.	E-Commu-nication	All the officials of the Institute will be allotted an email id under icsi.edu domain. All official communications with the outside world will be done by the officials through this email id only. All ROs/Chapters/CCGRT will be allotted an email id under icsi.edu domain. All official communications with the outside world on behalf of the ROs/Chapters/CCGRT may be issued through this email id.
4.	Maintenance of Hardware	Every Office of the Institute of its own will arrange the maintenance of hardware through local service providers. The Office will go for Annual Maintenance Contract with a suitable local Hardware Maintenance Firm for the same.

IV. GUIDELINES FOR THE USERS TO AVAIL IT RELATED SERVICES

The main objective for formulating the guidelines for the users to avail IT related services in the Institute is to provide for timely services and effective management and monitoring of the service levels. Such guidelines are applicable on all officials without exception. The guidelines are as under:

1. ***Bulk Mail*** – The User Directorate shall only use the respective option provided on COSMIC Sharepoint Portal. Request through any other mean shall be summarily rejected.

2. ***Bulk SMS*** – The User Directorate shall only use the respective option provided on COSMIC Sharepoint Portal. Request through any other mean shall be summarily rejected.

3. ***Website*** - The User Directorate shall only use the respective option provided on COSMIC Sharepoint Portal. Request through any other mean shall be summarily rejected.

4. ***Hardware Repair / Configuration / Upgradation / Movement*** –The Request shall only be catered through the Online Helpdesk to ensure control and monitoring. All users shall use the Online Helpdesk and monitor the progress through the same only. All other forms of complaints shall be summarily rejected.

   Action can be taken against any engineer associated with Directorate of IT in case any complaint is handled without it being recorded on the Online Helpdesk. The action may be disassociation with the support firm.

In case of the request for upgradation / movement of hardware from one place to another, the FMS engineer will get the requisite form filled by the User Directorate and thereafter initiate action. The completed form will be kept by the FMS Engineer for audit purpose.

5. ***Software Bugs*** – Any bug as identified in the software must be recorded on the Online Helpdesk and complaint no. should be recorded by the user. All other ways of request shall be summarily rejected.

6. Directorate of IT shall provide for services which are only referred to by the User Directorate through the Online Helpdesk. In exceptional circumstances and on the advice of CE, the request may be taken from any other source.

7. User Interface has been provided to all User Directorate to handle all types of queries. In case, any query where user interface is already available is forwarded to Directorate of IT, the same shall be summarily rejected.

8. In case of retired / left employees from the ICSI head quarter and Noida Office, the hardware assigned against the retired / left official will be returned back by the User Directorate to the Directorate of IT. Allocation / Reallocation of all hardware to the directorates will be through Directorate of IT only.

   For any request pertaining to return / allocation of hardware, the FMS engineer will get the requisite form filled by the User Directorate and thereafter initiate action. The completed form will be kept by the FMS Engineer for audit purpose (format Enclosed).

V. IT FACILITIES AND SERVICES FROM THE ICSI FOR THE STAKEHOLDERS

1. For Officials

Hardware

a) State of Art Data Center in ICSI Noida comprising of Racks, Servers, L2 Switches, L3 Switches, Routers, Firewalls, Storage devices, Wi-Fi Devices etc.

b) State of Art Data Center in ICSI HQ at Lodi Road, New Delhi comprising of Racks, Servers, L2 Switches, L3 Switches, Routers, Firewalls, Wi-Fi Devices etc.

c) Desktop or Laptop for use to all officials

d) Printers(Line Printer/Laser Printer/Dot Matrix Printer (DMP)/Deskjet Printer) and Scanners for all officials in the directorates on shared basis. Facility of Printer cum photocopier cum FAX machine to few directorates.

e) Facility of Colour Laser Printer to selected directorates.

Network

f) State of Art Local Area Network in ICSI Noida and ICSI HQ at Lodi Road, New Delhi.

g) State of Art Wide Area Network (WAN) / Virtual Private Network (VPN) connectivity between 12 Offices of the Institute (ICSI Noida (Hub), ICSI HQ, 4 ROs, CCGRT, Noida Chapter, Gurgaon Chapter, Jaipur Chapter, Pune Chapter, Hyderabad Chapter.

h) Internet Lease Line (ILL) for the users in ICSI Noida and ICSI HQ.

i) Full-fledged Wi-Fi network in ICSI Noida and ICSI HQ.

j) Well-structured IT Network Security through VLAN implementation at ICSI NOIDA and HQ.

Bulk Mailing and Bulk SMS Services (through Directorate of IT)

Disaster Recovery Site for Data Center to manage Business Continuity Process (BCP)

Any special exemption given to any ICSI employee from the following list shall stand revoked automatically on 31st Dec every year. All such privileges are provided on calendar year basis.

1) Complete Internet Access / opening of specific sites
2) USB Port Enabled.
3) Specific Applications/Folder access Permissions.
4) Any other IT Specific privileges.

The users who need any IT specific privileges may kindly submit their new User permission Request forms with the approval of their HOD before 31st December positively for continuity of any special exemption.

IT Help Desk Service for all offices under WAN (http://14.140.246.77:8080)

Centralised Call Center for The Institute's Stakeholders (Dial @ 011-33132333 from 7:00 A.M to 11:00 P.M)

Voice Communication

k) Intercom Connectivity through network between ICSI Noida and ICSI HQ

System Software & Office Automation Packages

l) Window Operating System for all

m) MS Office Software as Office Automation Package

n) Special DTP Software like Coreldraw, Page Maker to the Directorates as per the requirement.

o) SQL Server and Dot Net as the software development platform for IT.

p) Dot Net Nuke as the development platform for the Website.

q) Linux and Oracle as the ERP customization tool for IT.

r) Visual Source Safe (VSS) for managing the versions for programmers.

s) Visual Foxpro as Legacy Software Platform.

t) Semantic Anti-Virus Software

u) Manage Engine S/W Tool for Helpdesk.

v) OP Manager S/W Tool for DC Servers Health Monitoring.

w) Inmage and CA Arc Serv S/W Tool for Backup System

Application Software

x) Customised Application Software for the directorate users:

i) For Directorate of Student Services

- Registration Module

ii) Enrollment for Examination Module for Directorate of Examination

- Pre-Examination (Projection) Module
- Result Processing Module
- Result Verification Module

iii) For Directorate of Training & Membership

- Training Module
- Licentiate Module
- Membership Module
- Company Secretary Benevolent Fund (CSBF) Module

iv) For Directorate of Academics

- Chartered Secretary Subscription (CSS) Module

v) For Directorate Finance & Accounts

- Provident Fund Module

Enterprise Resource Planning (ERP)

y) Enterprise Resource Planning (ERP) system for the users in the selected application areas (Currently implemented for 28 offices):

- Finance & Accounts
- Payroll
- Employee Expenses Reimbursements (HQ only)
- Human Resource
- Inventory
- Purchase

z) ERP based self service to all officials.

aa) Receipt Accounting System (RAS) and Central Receipt Accounting System (CRAS) for all offices (Currently implemented in 40 offices).

Document Management System

bb) Sharepoint based File Management System for the Directorates/ROs/CCGRT/Chapters.

cc) Sharepoint based Knowledge Management System for the Directorates/ROs/CCGRT/Chapters.

dd) Workflow based online approval system for various claims.

ee) Workflow based request submission for various purpose such as bulk SMS/bulk mails.

Online Communication Services

ff) Online Communication facility through Office Communicator.

Online tutor / User Manual

gg) Online tutor / User Manual for various modules through Sharepoint Portal.

List of various user request forms download

All Employees of ICSI can download various user Request forms from COSMIC home page at Link: User Permission Forms Download.

- ICSI User Access Authorization(Creation/Deletion/Modification) Form version V2.0
- ICSI Folder and Application Permission Grant Revoke Request Form Version V2.0
- ICSI Password Reset Request Form Version V2.0
- ICSI Port Open Request Form Version V2.0
- ICSI Software Installation/Removal Request Form Version V2.0
- ICSI REQUEST FOR FUNCIONING OF THE SERVER ON HOLIDAYS Form Version V2.0
- ICSI User IT Clearance Form Version V2.0
- ICSI Attendance Record Form Version V1.0
- ICSI Feedback Record Form Version V1.0

Emailing System

hh) Email Id under icsi.edu domain to all officials.

ii) Email Id under icsi.edu domain to all ROs/Chapters/CCGRT.

jj) Email Id under icsi.edu domain to Council Members/Chairman & Secretary of Managing Committee of the RO/Chapters

Infrastructure in RO/Chapters/CCGRT

kk) IT Infrastructure (Hardware, Software & Internet) available in 4 Regional Offices (ROs), Center for Corporate Governance Research and Training (CCGRT) and most of the Chapters.

2. For Students, Members and others

a) Flood of information regarding the Institute and its services through the website www.icsi.edu.

b) Various Online services for the students, members and others through the website such as Registration, Enrollment, Placement, e-cart, e-tender, Membership, Grievance modules etc.

c) Payment gateway facility through Billdesk, Axis Bank, City Bank, Techprocess Payment gateway systems and Online Payment through Challan System.

d) Online Admit Card and Result with E- Mark Sheet (for Foundation and Executive Programmes) on third party portal through the Institute's website.

e) Facility of online registration on the website for result through mail.

f) Facility of E-learning (http://elearning.icsi.edu).

VI. UNIFORMITY NETWORK POLICY FOR RO/ CCGRT / CHAPTERS

Objective: To ensure that a proper balance is maintained between the IT infrastructure and the manpower using this infrastructure, ensure uniform specification and configurations in the whole system keeping in view the IT initiatives being implemented by ICSI HQ, the IT Committee of the Institute has felt the need of a uniform networking policy to be adopted by the RO/CCGRT/Chapters.

Network Policy in details:

Local Area Network (LAN):

- Offices having 2 or more desktops can implement LAN.
- LAN should be built with CAT 6 cables and Switches of reputed brands like D-Link, CISCO etc.
- One time cost for LAN implementation will be reimbursed by HQ
- Maintenance charges for LAN implementation is to be borne by the respective RO/CCGRT/Chapter.

Wide Area Network (WAN):

- RO/CCGRT/Chapters are not allowed for establishing WAN of its own.
- ICSI HQ will take care of the WAN connectivity for RO/CCGRT/Chapters as per the direction of the IT Committee of the Institute.
- WAN connectivity will be initially implemented in ROs/CCGRTs with 3 MBPS bandwidth and in Chapters with 1 MBPS bandwidth.
- VPN bandwidth may be further upgraded in ROs/CCGRTs/Chapters as per the requirement. But the bandwidth charges up to 5 MBPS for ROs/CCGRT and 2 MBPS for Chapters will only be borne by the ICSI HQ and for upgradation of bandwidth beyond this limit, the charges will be borne by the respective RO/CCGRT/Chapter Office.

Internet connectivity:

- RO/CCGRT/Chapters have to take internet connectivity compulsorily provided they are using desktops.
- Internet connectivity is to be taken by RO/CCGRT/Chapter from a reputed local internet service providers like BSNL, VSNL, MTNL, Tata, Airtel, Reliance etc.
- RO/CCGRT/Chapters are free to procure any internet plan as per their requirements.
- The cost for Internet connectivity will be borne by respective RO/CCGRT/ Chapter.

Wi-Fi Connectivity

- RO/CCGRT/Chapter may implement Wi-Fi connectivity as per their requirement.
- Wi-Fi connectivity is to be taken by RO/CCGRT/Chapter from a reputed local service providers like BSNL, VSNL, MTNL, Tata, Airtel, Reliance etc.
- RO/CCGRT/Chapters are free to procure Wi-Fi plan as per their requirements.
- The one time amount for Wi-Fi implementation will be reimbursed by HQ.
- The Maintenance charges for the Wi-Fi connectivity is to be borne by the respective RO/CCGRT/Chapter

VII. INTERNET USAGE GUIDELINE FOR USING THE INTERNET FACILITY BY THE EMPLOYEES IN RO/CCGRT/CHAPTERS

- The display of any kind of sexually explicit image or document on any ICSI system is expressly prohibited. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
- No employee may use ICSI facilities knowingly to download or distribute pirated software or data.
- No employee may use the ICSI's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap door program code.
- No employee may use the ICSI's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential information like employee information, customer data and trade secrets.
- Employees with Internet access must not use ICSI Internet facilities to download software or games, or to play games against opponents over the Internet, download images or videos unless there is an explicit business-related use for the material.
- Employees with Internet access may not upload any software licensed to ICSI or data owned or licensed by ICSI without explicit authorization from the manager responsible for the software or data.
- ICSI has installed firewalls, proxy servers, and Internet address screening programs to assure the safety and security of the Institute networks. Any employee who attempts to disable, defeat or circumvent any ICSI security facility will be subject to immediate dismissal.
- Employees are provided with internet access only for business purposes in interest of the institute. Any personal chats and other personal web emails, except ICSI provided emails are strictly prohibited.
- Every employee will be provided with internet connection facility on his/her desktop.
- Employees may be restricted to use the selected sites such as yahoo, Gmail, banks etc. during office hours OR completely. However the usage of certain sites may be opened for those staff, who have to use the same for official purpose. Such employees are required to forward the requisite privilege form duly signed by his/her HOD to the Directorate of IT.

VIII. Compliances for RO/CO/CCGRT (Points to note)

- Software License Compliance to be made. RO/CO/CCGRT has to submit yearly Software License Compliance declaration certificate to DIT.
- Regular Updation of Child Portal needs to be done. RO/Chapter/CCGRT has to submit monthly compliance report to DIT.
- RO/CO/CCGRT have to use email id under icsi.edu domain
- RO/CO/CCGRT has to procure hardware within max. 30 days after receiving approval from HQ
- New Chairman and Secretaries of RC/MC have to submit their declaration certificate to DIT for issuing emails id under icsi.edu domain
- RO/CO/CCGRT should bring all hardware under AMC
- RO/CO/CCGRT/Directorates should submit their request for bulk mailing / Bulk SMS / Website Updation to DIT before at least 3 working days
- RO/CO/CCGRT should submit Monthly MIS on IT to DIT by 7th day of every month
- RO/CO/CCGRT/Directorates should nominate Website Nodal Officer.
- RO/CO/CCGRT should form IT Committee to look after the IT activities
- All officials should lodge Complaints in IT helpdesk i.e. https://helpdesk.icsi.edu
- RO/CO/CCGRT should maintain Cash/Cheque/DD receipts in CRAS
- RO/CO/CCGRT should carry out CRAS reconciliation on daily basis
- RO/CO/CCGRT should maintain all financial and inventory transaction in ERP
- RO/CO/CCGRT should carry out financial and inventory reconciliation on monthly basis.

IX. GUIDELINES RELATED TO BULK MAIL/SMS/ WEBSITE UPDATION

a) RO/CO/CCGRT/Directorates should nominate one Nodal Officer for the activities related to Bulk Mail/SMS/Website Updation and inform Directorate of IT. All requests pertaining to Bulk Mail/SMS/Website Updation should be moved to Directorate of IT by the Nodal Officer only.

b) Every request from the Nodal Officer should be for single activity i.e. for either bulk mail or bulk SMS or Website Updation. Multiple activities should not be proposed through a single request. Such type of request will not be entertained / considered.

c) After receiving the request from the user related to Bulk Mail/SMS, the dealing official from Directorate of IT will prepare a draft pertaining to the requested activity and send it to the user for approval. It is the responsibility of the user to verify and approve the draft before sending it to the stakeholders. Bulk email/ SMS shall not be sent without receipt of approval of draft.

d) After receiving the request from the user related to Website Updation, the dealing Official from Directorate of IT will do the needful on the Website and inform the user to verify and confirm. If no reply is received from the user, it will be assumed that the needful done is correct.

e) Any request pertaining to Bulk Mail/SMS and Website Updation received from the user after office hours will be dealt / entertained on next Working day only. If the matter is of urgent in nature, it should be sent to Directorate of IT with the approval of CE & OS. Further the matter should be informed telephonically to Directorate of IT.

THE INSTITUTE OF
Company Secretaries of India
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament

Headquarters
ICSI House, 22, Institutional Area, Lodi Road, New Delhi 110 003
tel 011- 4534 1000, 4150 4444 **fax** 24626727
email info@icsi.edu **website** www.icsi.edu / www.icsi.in